

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-222172

(P2002-222172A)

(43) 公開日 平成14年8月9日 (2002.8.9)

(51) Int.Cl. ⁷	識別記号	F I	テ-マ-ト* (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 C 5 B 0 8 5
13/00	5 1 0	13/00	5 1 0 A 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 A

審査請求 有 請求項の数 2 O L (全 7 頁)

(21) 出願番号 特願2001-17207(P2001-17207)

(22) 出願日 平成13年1月25日 (2001.1.25)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 中川 広一

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(72) 発明者 入江 一成

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外2名)

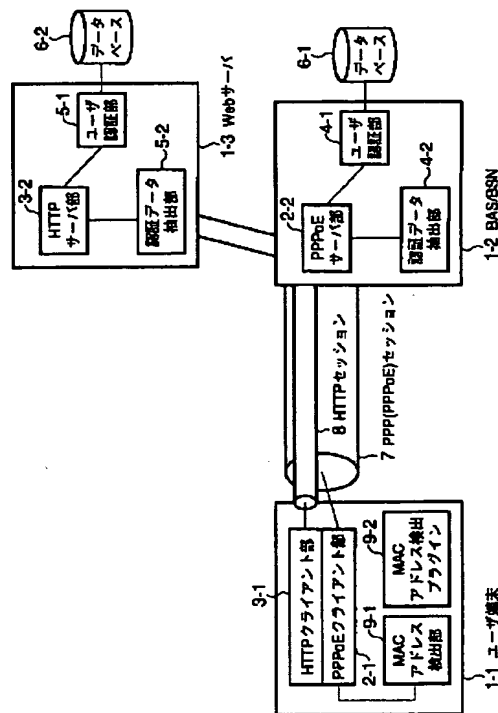
最終頁に続く

(54) 【発明の名称】 ユーザ認証方法

(57) 【要約】

【課題】 本発明の課題は、MACアドレスも認証パラメータとして用いることにより、セキュリティの高いユーザ認証方法を提供することにある。

【解決手段】 本発明は、MACアドレス検出部9-1を有するユーザ端末1-1のPPPoEクライアント部2-1から、接続要求時にユーザ名とパスワードとMACアドレスをPPPoEフレーム内のPPPフレームの内部データの一部としてセンタ側へ送出し、PPPoEサーバ部2-2を有するセンタ側で、PPPoE内のPPPフレームの内部データからユーザ名とパスワードとMACアドレスを抽出し、抽出されたユーザ名とパスワードとMACアドレスを認証データベースと照合し、一致した場合にのみ接続を許可することを特徴とする。



【特許請求の範囲】

【請求項1】 MACアドレスを検出するMACアドレス検出部を有する端末側のPPPοEクライアント部から、接続要求時にユーザ名とパスワードとMACアドレスをPPPοEフレーム内のPPPフレームの内部データの一部としてセンタ側へ送出するステップと、PPPοEサーバ部を有するセンタ側で、PPPοE内のPPPフレームの内部データからユーザ名とパスワードとMACアドレスを抽出するステップと、前記ステップで抽出されたユーザ名とパスワードとMACアドレスを認証データベースと照合し、一致した場合にのみ接続を許可するステップとを有することを特徴とするユーザ認証方法。

【請求項2】 MACアドレスを検出するMACアドレス検出部を有する端末側のHTTPクライアント部から、Webサイトへの接続要求時にユーザ名とパスワードとMACアドレスをHTTPフレームの内部データの一部としてセンタ側へ送出するステップと、HTTPサーバ部を有するセンタ側で、HTTPフレームの内部データからユーザ名とパスワードとMACアドレスを抽出するステップと、前記ステップで抽出されたユーザ名とパスワードとMACアドレスを認証データベースと照合し、一致した場合にのみ接続を許可するステップとを有することを特徴とするユーザ認証方法。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】本発明は、通信回線を介してユーザ端末（パソコン）とネットワークサイドのサーバ（コンピュータ）間の通信を行うコンピュータ通信システムにおいて、セキュリティの高いウェブ（Web）アクセスやコンテンツダウンロードを提供するためのMAC（Media Access Control）アドレスを用いたユーザ認証方法に関するものである。

【0002】

【従来の技術】これまで通信回線を介してコンピュータ間の通信を行うための様々なシステムが開発されている。コンピュータ通信のうち、IP（Internet Protocol）プロトコルを用いるものはインターネットあるいはエキストラネットとして広く普及してきた。通信インフラとしては、電話回線を利用したダイヤルアップによるモデム通信、CATV回線に接続されたモデムにより通信を行うケーブルモデムシステム、無線回線あるいは光ファイバを利用したシステムが開発されている。近年特に、従来からのメタリック電話回線を共用してデータ通信が可能なADSL（Asymmetric Digital Subscriber Loop）が注目されている。これはユーザ側にATUと呼ばれるADSL終端装置、センタ側にはDSLAM（ADSL Access Multiplexer）と呼

ばれる装置を設置し、さらにその先にBAS（Broadband Access Server）あるいはBSN（Broadband Service Node）と呼ばれるノード装置を設置し、ユーザを収容する。

【0003】現在、ADSLではIP通信を行うために、ユーザ端末からBASまでをブリッジモードで接続し、イーサネット（登録商標）（Ethernet（登録商標））上でPPP（Point-to-Point Protocol）を用いる、PPPοE（PPP over Ethernet）が利用されている。一般的にPPPでは、ユーザ名、パスワードを用いて、認証を行っている。しかし、他人にユーザ名とパスワードが漏洩した場合は、本人でなくとも接続が可能となり、ユーザ名とパスワードのみの認証では、本人であることの確認が不十分である。

【0004】また、同様に、インターネット普及のクライアントアプリケーションとなったWWW（World Wide Web）における認証においても一般的にユーザ名とパスワードによってサイトへの接続認証が行われている。この場合も、他人にユーザ名とパスワードが漏洩することで、本人でなくとも当該サイトに接続が可能となる。

【0005】このようにユーザ名とパスワードのみによる認証は他人によるなりすましを防ぐことができないと言う問題があった。

【0006】従来のPPP接続におけるユーザ認証方法の1例を図6及び図7に示す。図6は一般的なユーザ認証システム構成図であり、図7は図6のユーザ認証システムにおける処理フロー示している。図中、1-1はユーザ端末、1-2はBASあるいはBSN、1-3はWebサーバ、2-1はPPPοEクライアント部、2-2はPPPοEサーバ部、3-1はHTTP（Hypertext Transfer Protocol）クライアント部、3-2はHTTPサーバ部、4-1はPPPにおけるユーザ認証部、5-1はHTTPにおけるユーザ認証部、6-1、6-2は認証データベース、7はPPP（PPPοE）セッション、8はHTTPセッションを示す。また図示しないが、ユーザ端末1-1とBAS1-2のあいだにATUとDSLAMが設置される。ユーザ端末1-1とATUはEthernet接続、ATUとDSLAMはADSL回線接続、DSLAMとBAS1-2はATM専用線による接続が一般的である。

【0007】ユーザ端末1-1がWebサーバ1-3へアクセスするために、PPPοEクライアント部2-1が起動し、PPPοEクライアント部2-1とPPPοEサーバ部2-2との間でPPPセッション7を確立しようとする。そのために、ユーザは「ユーザ@Realm名」と「パスワード」を入力し、BAS1-2内のユ

ーザ認証部4-1にデータを渡し、認証データベース6-1と照合を行い認証を行う。ユーザデータが正しければ、PPP (PPPoE) セッション7を確立する。その後、HTTPクライアント部3-1はHTTPサーバ部3-2との間で通信を行う。この場合、認証に必要なHTTPサーバ部3-2へ接続するために、HTTPクライアント部3-1から入力されたユーザ名、パスワードをユーザ認証部5-1で認証データベース6-2と照合して認証を行う。

【0008】このようにユーザ名とパスワードのみで認証するのが一般的である。そのため、ユーザ名、パスワードの漏洩によって、他人によるなりすましが起こるという問題があった。

【0009】

【発明が解決しようとする課題】上記のように従来の技術を用いた方式では、PPP (PPPoE) セッションを確立する際と認証に必要なHTTPサーバ部へ接続する際において、ユーザ名とパスワードのみで認証を行うため、接続してくるユーザが本人であるか確認することができず、なりすましが可能であった。

【0010】本発明は上記の事情に鑑みてなされたもので、PPP (PPPoE) でセッションを確立し、そのセッション上でHTTPプロトコルによってデータの送受信を行う通信において、NIC (Network Interface Card) ごとに一意であるMACアドレスも認証パラメータとして用いることにより、セキュリティの高いユーザ認証方法を提供することを目的とする。

【0011】

【課題を解決するための手段】上記目的を達成するために本発明のユーザ認証方法は、MACアドレスを検出するMACアドレス検出部を有する端末側のPPPoEクライアント部から、接続要求時にユーザ名とパスワードとMACアドレスをPPPoEフレーム内のPPPフレームの内部データの一部としてセンタ側へ送出するステップと、PPPoEサーバ部を有するセンタ側で、PPPoE内のPPPフレームの内部データからユーザ名とパスワードとMACアドレスを抽出するステップと、前記ステップで抽出されたユーザ名とパスワードとMACアドレスを認証データベースと照合し、一致した場合にのみ接続を許可するステップとを有することを特徴とする。

【0012】また本発明のユーザ認証方法は、MACアドレスを検出するMACアドレス検出部を有する端末側のHTTPクライアント部から、Webサイトへの接続要求時にユーザ名とパスワードとMACアドレスをHTTPフレームの内部データの一部としてセンタ側へ送出するステップと、HTTPサーバ部を有するセンタ側で、HTTPフレームの内部データからユーザ名とパスワードとMACアドレスを抽出するステップと、前記ス

テップで抽出されたユーザ名とパスワードとMACアドレスを認証データベースと照合し、一致した場合にのみ接続を許可するステップとを有することを特徴とする。

【0013】

【発明の実施の形態】以下図面を参照して本発明の実施形態例を詳細に説明する。

【0014】図1は本発明の実施形態例を示すシステム構成図、図2は本発明の実施形態例に係るPPPoEにおける認証機能のレイヤ構成図、図3は本発明の実施形態例に係るPPPoEにおける認証の処理フローを示すシーケンス図、図4は本発明の実施形態例に係るHTTPにおける認証機能のレイヤ構成図、図5は本発明の実施形態例に係るHTTPにおける認証の処理フローを示すシーケンス図である。

【0015】図中、1-1はユーザ端末、1-2はBASあるいはBSN、1-3はWebサーバ、2-1はPPPoEクライアント部、2-2はPPPoEサーバ部、3-1はHTTPクライアント部、3-2はHTTPサーバ部、4-1はPPPにおけるユーザ認証部、4-2はPPPoEサーバ部における認証データ抽出部、5-1はHTTPにおけるユーザ認証部、5-2はHTTPサーバ部における認証データ抽出部、6-1、6-2は認証データベース、7はPPP (PPPoE) セッション、8はHTTPセッション、9-1はNICごとに設定されているMACアドレスを検出するMACアドレス検出部、9-2はNICごとに設定されているMACアドレスを検出するMACアドレス検出プラグイン (Plugin)、10-1、10-2、10-3、10-4は物理レイヤ、11-1はユーザ端末側のPPPレイヤ、11-2はBASあるいはBSN側のPPPレイヤ、12-1はユーザ端末側のHTTPレイヤ、12-2はWebサーバ側のHTTPレイヤ、13-1、13-2はPPPoEレイヤ、14-1、14-2はTCP/IPレイヤを示す。なお図示しないが、ユーザ端末1-1とBAS1-2のあいだにATUとDSLAMが設置される。ユーザ端末1-1とATUはEthernet接続、ATUとDSLAMはADSL回線接続、DSLAMとBAS1-2はATM専用線による接続が一般的である。

【0016】実施形態例1 (PPPoEクライアント、サーバがMACアドレスを認証に用いる場合) : 図1の構成図において、PPPoEクライアント部2-1でPPPoEサーバ部2-2に接続するとき、図3に示すように、ユーザは、PPPoEクライアント部2-1を起動し、PPPoEクライアント部2-1に対しPPPoEサーバ部2-2への接続要求を行う。PPPoEサーバ部2-2はPPPoEクライアント部2-1に認証要求を送る。PPPoEクライアント部2-1は、MACアドレス検出部9-1によりユニックス (Unix) の ifconfig コマンドやウィンドウズ (登録商標)

(Windows) の ipconfig コマンドに該当する機能を用いて、図2に示すように、物理レイヤ10-1から当該ユーザパソコンのMACアドレスを取得する。MACアドレス検出部9-1は、PPP/Eクライアント部2-1にMACアドレスを渡し、PPP/Eクライアント部2-1は、ユーザが入力した「ユーザ@realm名」、「パスワード」、及び自動検出した「MACアドレス」の認証情報をPPP (PPP/E) フレームに格納し、PPP/Eサーバ部2-2に送出する。

【0017】PPP/Eサーバ部2-2の認証データ抽出部4-2は、PPP/Eクライアント部2-1から送られた認証情報から「ユーザ@realm名」、「パスワード」、「MACアドレス」の認証データを取り出して、ユーザ認証部4-1が認証データを認証データベース6-1に送出し、照合する。認証データのすべてが一致した場合はユーザが認証(認証1)されたとみなし、PPP/Eクライアント部2-1とPPP/Eサーバ部2-2の間でPPP (PPP/E) セッション7を確立する。

【0018】実施形態例2 (HTTPクライアント、サーバがMACアドレスを認証に用いる場合) : PPP/Eクライアント部2-1は、PPP/Eクライアント部2-1を起動し、ユーザが入力した「ユーザ@realm名」と「パスワード」をPPP (PPP/E) フレームに格納し、PPP/Eサーバ部2-2に送出する。PPP/Eサーバ部2-2では従来方式どおり「ユーザ@realm名」と「パスワード」を用いて認証(認証1)を行い、PPP (PPP/E) セッション7を確立する。

【0019】HTTPクライアント部3-1は、PPP (PPP/E) セッション7上で、HTTPセッション8を確立し、HTTPクライアント部3-1とHTTPサーバ部3-2が通信を行う。HTTPクライアント部3-1とHTTPサーバ部3-2間で認証が必要な場合が発生した場合、本発明では、以下のような認証を行う。

【0020】図1で、HTTPクライアント部3-1はHTTPサーバ部3-2に接続するとき、ユーザはHTTPクライアント部3-1に対しHTTPサーバ部3-2への接続要求を行う。図5に示すように、HTTPサーバ部3-2はHTTPクライアント部3-1に認証要求を送る。ユーザはHTTPクライアント部3-1に対して、「ユーザ名」、「パスワード」を入力し、HTTPクライアント部3-1はMACアドレス検出要求をし、図4に示すように、MACアドレス検出プラグイン(Plugin) 9-2により物理レイヤ10-3から当該ユーザパソコンのMACアドレスを自動検出して取得する。MACアドレス検出プラグイン(Plugin) 9-2は、HTTPクライアント部3-1にMACアドレスを渡し、HTTPクライアント部3-1は、

「ユーザ名」、「パスワード」、「MACアドレス」の認証情報をHTTPフレームに格納し、HTTPサーバ部3-2へ送出する。

【0021】HTTPサーバ部3-2の認証データ抽出部5-2は、HTTPクライアント部3-1から送られた認証情報から「ユーザ名」、「パスワード」、「MACアドレス」の認証データを取り出し、認証データを認証データベース6-2と照合する。認証データのすべてが一致した場合はユーザが認証(認証2)されたとみなし、HTTPクライアント部3-1とHTTPサーバ部3-2間でHTTPセッション8を確立し、アクセス可能にして通信が行われる。

【0022】実施形態例3 (PPP/E, HTTPともにMACアドレスを認証に用いる場合) : 上記、実施形態例1と実施形態例2を同時に行うことで、PPP/EによるPPP (PPP/E) セッション確立時とHTTPによるセッション確立時にMACアドレスを用いた認証を行う。

【0023】

【発明の効果】以上述べたように本発明によれば、NICごとに一意であるMACアドレスを認証に用いることにより、ユーザ認証におけるセキュリティを高め、なりすましを防ぐ効果がある。

【図面の簡単な説明】

【図1】本発明の実施形態例を示すシステム構成図である。

【図2】本発明の実施形態例に係るPPP/Eにおける認証機能のレイヤ構成図である。

【図3】本発明の実施形態例に係るPPP/Eにおける認証の処理フローを示すシーケンス図である。

【図4】本発明の実施形態例に係るHTTPにおける認証機能のレイヤ構成図である。

【図5】本発明の実施形態例に係るHTTPにおける認証の処理フローを示すシーケンス図である。

【図6】従来のユーザ認証システム構成の一例を示すブロック図である。

【図7】従来のユーザ認証方法における処理フローの一例を示すシーケンス図である。

【符号の説明】

- 1-1 ユーザ端末
- 1-2 BASあるいはBSN
- 1-3 Webサーバ
- 2-1 PPP/Eクライアント部
- 2-2 PPP/Eサーバ部
- 3-1 HTTPクライアント部
- 3-2 HTTPサーバ部
- 4-1 PPPにおけるユーザ認証部
- 4-2 PPP/Eサーバ部における認証データ抽出部
- 5-1 HTTPにおけるユーザ認証部
- 5-2 HTTPサーバ部における認証データ抽出部

6-1, 6-2 認証データベース

7 PPP (PPPoE) セッション

8 HTTPセッション

9-1 MACアドレス検出部

9-2 MACアドレス検出プラグイン (Plugin)

10-1, 10-2, 10-3, 10-4 物理レイヤ

11-1 ユーザ端末側のPPPレイヤ

11-2 BASあるいはBSN側のPPPレイヤ

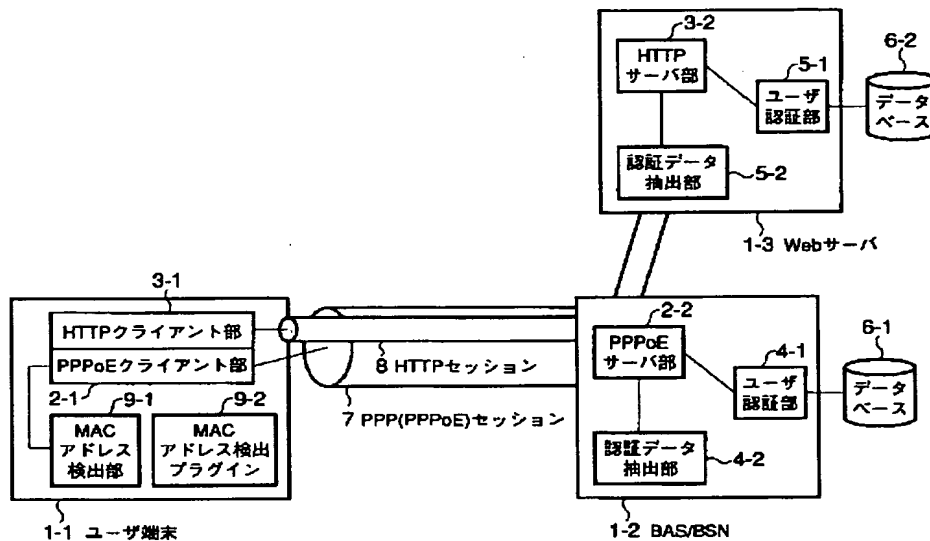
12-1 ユーザ端末側のHTTPレイヤ

12-2 Webサーバ側のHTTPレイヤ

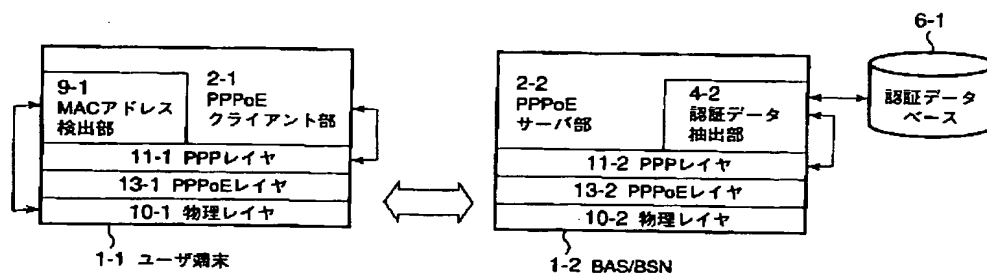
13-1, 13-2 PPPoEレイヤ

14-1, 14-2 TCP/IPレイヤ

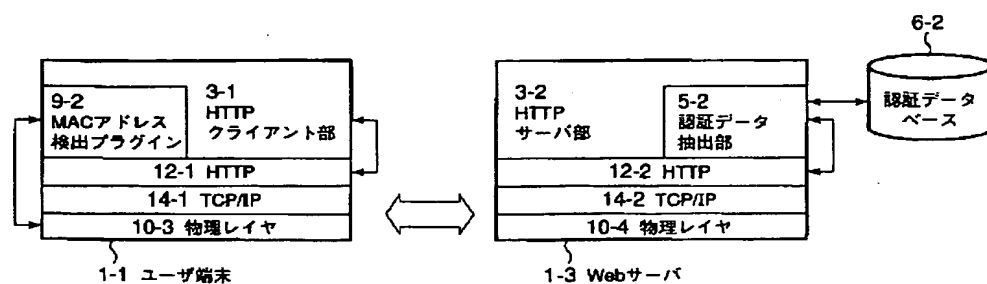
【図1】



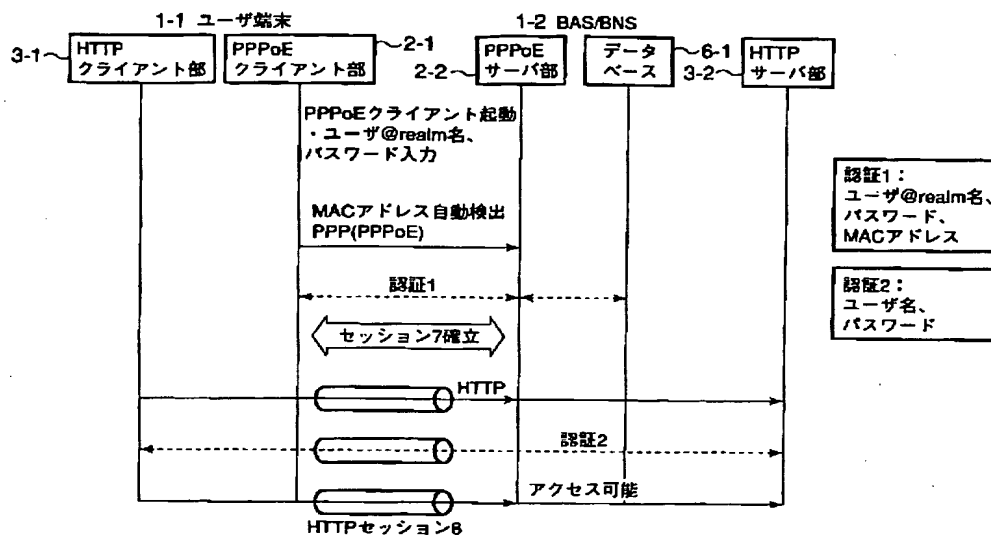
【図2】



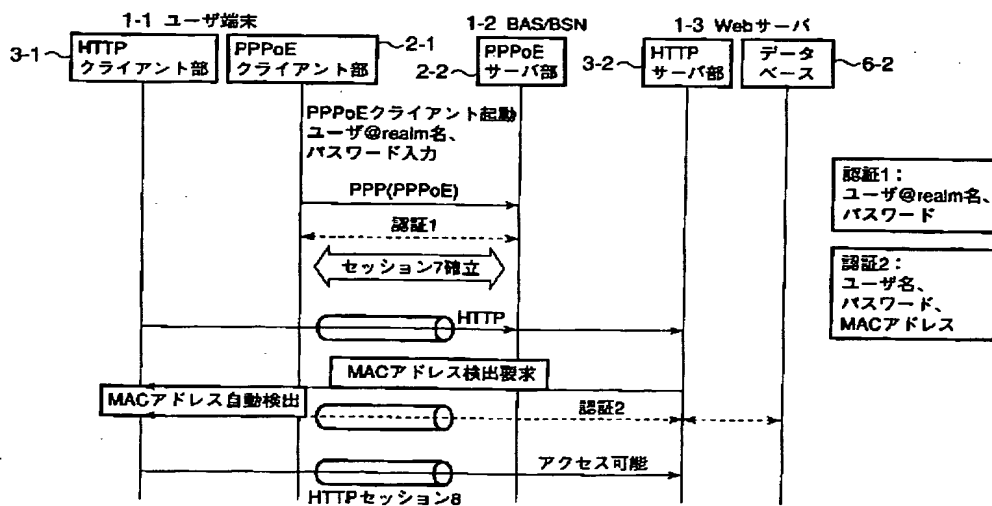
【図4】



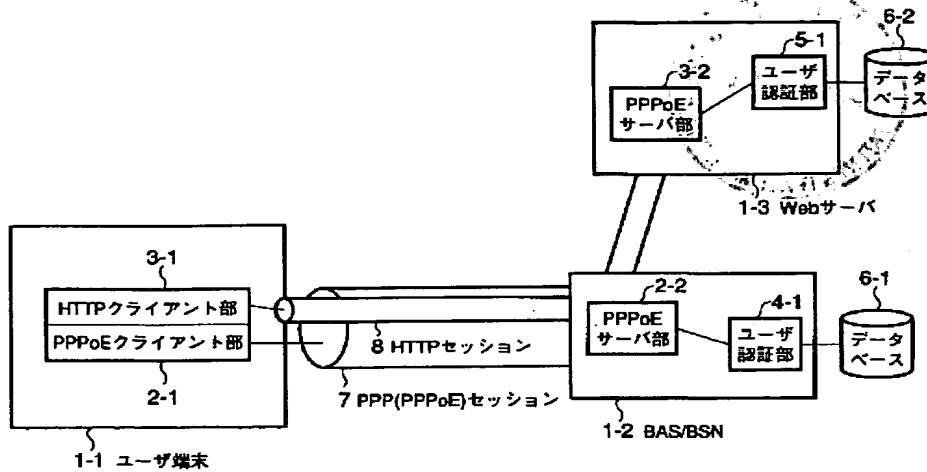
【図3】



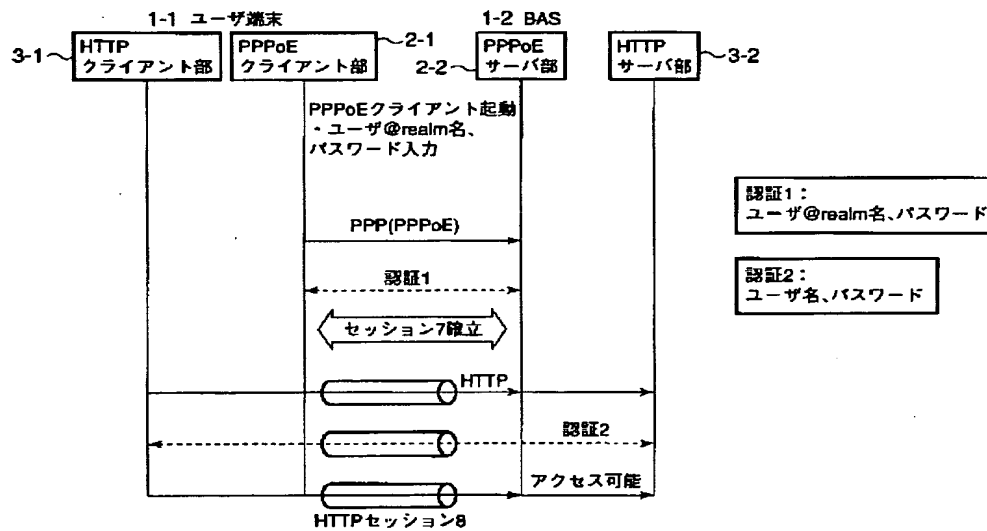
【図5】



【図6】



【図7】



フロントページの続き

(72)発明者 佐々木 将人
東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内

(72)発明者 渡瀬 順平
東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内
Fターム(参考) 5B085 AE04 AE23 BG07
5J104 AA07 KA01 NA05 PA07